REMARKS

The Office Action dated October 17, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Status of the Claims

Claims 1, 3-8, 10, 13, 16, 17, 20, 21, 30, 31 and 34-37 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter has been added. Claims 1, 3-8, 10-21 and 29-37 are currently pending in the application and are respectfully submitted for consideration.

Allowable Subject Matter

Applicants note with appreciation the Examiner's indication that claims 4, 5, 11, 16-18, 30 and 31 would be allowable if rewritten in independent form. Applicants kindly thank the Examiner for the assistance. Applicants also respectfully submit that claim 32 should also be allowable because, while having its own scope, claim 32 recites similar features to allowable claim 18. Applicants respectfully submit that the remaining pending claims also patentably distinguish over the cited art for at least the reasons discussed below.

Rejection under 35 U.S.C. § 102

Claims 1, 3, 6-8, 10, 12-15, 19-21, 29 and 32-37 were rejected under 35 U.S.C. §102(e) as allegedly being anticipated by Kennedy et al. (U.S. Publication No. 2004/0252683). The Office Action took the position on page 2 that Kennedy et al.

teaches all of the features of the rejected claims. Applicants respectfully traverse the rejection. Reconsideration of the claims is respectfully requested.

Independent claim 1, from which claims 3-8 and 10-12 depend, recites a method including receiving a message from a terminal device connected to a packet data network, deriving first source information from the message and deriving second source information. The method also includes comparing the first source information and the second source information, initiating protection processing based on a result of the comparing and providing secure access to the packet data network based on the protection processing.

Independent claim 13, from which claims 14-20 and 29-35 depend, recites an apparatus including a receiving unit configured to receive a message from a terminal device connected to the network element and a deriving unit configured to derive first source information from the message and to derive second source information. The apparatus also includes a comparing unit configured to compare the first source information and the second source information and a protecting unit configured to initiate protection processing based on a comparing result of the comparing unit and to provide secure access to a packet data network based on the protection processing.

Independent claim 36 recites an apparatus including receiving means for receiving a message from a terminal device connected to a network element and deriving means for deriving first source information from the message and for deriving second source information. The apparatus also includes comparing means for comparing the first source information and the second source information and protecting means for initiating protection

processing based on a comparing result of the comparing means and for providing secure access to a packet data network based on the protection processing.

Independent claim 37 recites a computer program embodied on a computer-readable storage medium configured to control a processor to perform operations, including receiving a message from a terminal device connected to a packet data network, deriving first source information from the message and deriving second source information. The operations also include comparing the first source information and the second source information, initiating protection processing based on a result of the comparing and providing secure access to the packet data network based on the protection processing.

As will be discussed below, Kennedy et al. fails to disclose or suggest all of the features of the above-rejected claims.

Kennedy et al. generally discusses "systems, methods, and computer program products for resolving addressing in networks that include a network address translator" (paragraph [0003]).

> A determination is made upon the initiation of a communication session as to whether one or more of the nodes included in the session are behind a NAT. Based on the determination, information is exchanged from an independent application server to the nodes included in the session so as to resolve the addressing problems introduced by the NAT. The [alleged] invention is applicable in applications including, but not limited to, IP telephony, and applications complying with the session initiation protocol (SIP).

(Paragraph [0014] of Kennedy et al.).

Independent claim 1 recites, in part, "comparing said first source information and said second source information" and "initiating protection processing based on a result of

said comparing". Independent claims 14, 36 and 37, which each have their own scope, recite similar features. In rejecting these features, the Office Action broadly cited to paragraphs [0062]-[0067] of Kennedy et al. Applicants respectfully submit that Kennedy et al. fails to disclose or suggest these features.

Kennedy et al. discusses "a through which an application server 105 determines whether client A 101 and/or client B 103 are behind a network address translator (NAT)" (paragraph [0033]). In step S203, "the application server 105 determines whether the internal IP address and port sent by the client 101, 103 matches the IP source address and port that the application server 105 extracted from the header of the message originated by the client 101, 103" (*Id.*). Applicants submit that thereafter, the application server 105 merely determines whether or not the client 101, 103 is behind the network address translator based on the comparison result (see paragraphs [0033]-[0035] of Kennedy et al.). Paragraphs [0013] and [0014] of Kennedy et al. refer to an alleged security advantage of performing the address resolution. Based on the determination whether one or more of the nodes included in the session are behind a network address translator, information is exchanged so as to resolve addressing problems introduced by the network address translator.

On the other hand, the independent claims recite that protection processing is performed. In some embodiments of the present invention, for example, the protection processing may include deciding on whether to forward or not forward/drop a message depending on a comparison result. No such "protection processing" is performed in

Kennedy et al. Rather, per the above, the application server 105 of Kennedy et al. merely determines whether the internal IP address and port sent by the client 101, 103 matches the IP source address and port that the application server 105 extracted from the header of the message originated by the client 101, 103.

Per the above, Applicants note that the Office Action cited paragraphs [0062-0067] of Kennedy et al. as allegedly anticipating the above-recited features of claim 1. However, as noted in the previous Response filed July 15, 2008, these paragraphs do not disclose or suggest, for example, a protection processing based on the result of a comparison of a first source information derived from a received message of a terminal device and a derived second source information. Instead, these paragraphs discuss a calling sequence for performing NAT address resolution in a SIP application, primarily for avoiding delays in multimedia session communications. For this purpose, the system discussed in Kennedy et al. exchanges special messages between different network nodes on behalf of the controller, where additional fields (headers, cf. paragraphs [0065-0066]) containing IP addresses are added to messages. By comparing these IP addresses, the controller determines whether one or more nodes included in a session are behind a network address translator.

In contrast thereto, some embodiments of the present invention provide secure network access **without using additional fields and without sending additional special messages**. Due to the fact that the "comparison" of the present application is based on source information derived from an existing message itself or from source information

available at the concerned "protection" element of the network, there is **no need** for the involved network elements to send additional special messages with added fields.

Claims 3, 6-8, 10, 12, 13, 15, 19-21, 29 and 32-35 depend from independent claims 1 or 14 and add further features thereto. Thus, the arguments above with respect to the independent claims also apply to the dependent claims.

Per the above, Kennedy et al. fails to disclose or suggest all of the features of the above-rejected claims under 35 U.S.C. § 102(e). Accordingly, it is respectfully submitted that the rejection is overcome and respectfully requested that the rejection be withdrawn.

Conclusion

For at least the reasons presented above, it is respectfully submitted that the above-rejected claims are allowable over the cited art. Accordingly, it is respectfully requested that the claims be allowed and the application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

/ml at JTO (Reg. No. 60,180)

for Jared T. Olson
Attorney for Applicants
Registration No. 61,058

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

JTO:skl